UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

89441 7590 12/09/2009

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 12/09/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

TITLE OF INVENTION: PUBLIC KEY ENCRYPTION WITH DIGITAL SIGNATURE SCHEME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	03/09/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

89441 7590 12/09/2009

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

TITLE OF INVENTION: PUBLIC KEY ENCRYPTION WITH DIGITAL SIGNATURE SCHEME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	03/09/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
TESLOVICH, TAMARA	2437	713-180000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

89441 7590 12/09/2009

Jones Day (RIM) - 2N
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 12/09/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 569 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 569 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Notice of Allowability	Application No.	Applicant(s)	
	09/594,368	LITTLE, HERB A.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Applicant's After Final Amendments and Remarks*.

2. ☒ The allowed claim(s) is/are *1-8, 10-23, 25-38, 40-45*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

This Office Action is in response to Applicant's After Final Remarks and Amendments filed November 19, 2009.

Claims 9, 24, and 39 are cancelled.

Claims 1-8, 10-23, 25-38 and 40-45 are pending and herein considered.

Response to Arguments

The Examiner respectfully disagrees with Applicant's arguments concerning the entrance and consideration of Applicant's After Final remarks and amendments "because the assignee did not previously amend the claims in reliance on the examiner's confirmation, later retracted, that Schneier does not disclose ephemeral keys." Assignee was informed in their interview that while their oral remarks appeared persuasive, such remarks would need to be submitted formally for reconsideration before any decision regarding allowable subject would be made. Unfortunately for Applicants, it was during the Examiner's reconsideration of Applicant's remarks that she located within previously cited portions of Schneier specific support for the use of ephemeral key pairs. Insofar as Applicant was clearly in possession of the cited portions of Schneier before, during, and after their interview, the Examiner's response was not without fair notice. However, it is in view of Applicant's ample amendments that the Examiner has opted to reopen examination of the claims resulting in the finding of allowable subject matter described below.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Matt Johnson on December 4, 2009.

The application has been amended as follows:

This listing of claims will replace all prior versions, and listings of claims in the application:

1. (Currently Amended) A public-key encryption process for communicating messages between a sender device and a receiver device, comprising the steps of:

for each message:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver;

Deleted: and

b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step, wherein the digital signature comprises a first value *r* and a second value *s*; and

Deleted: wherein the ephemeral key pair used in the encrypting and generating steps is used for a single message between the sender and the receiver

c) transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;

wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X*, and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*.

2. (Original) A public-key encryption process according to claim 1, wherein the encrypting step uses an El Gamal encryption scheme.

3. (Previously Presented) A public-key encryption process according to claim 1, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme;

wherein the step of generating the digital signature includes hashing the plaintext message.

4. (Currently Amended) A public-key encryption process according to claim 1, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key *x* and calculating [[an]]the encryption ephemeral public key $X = xG$[[,]] in a finite cyclic group having *G* as a generator.

Deleted: where
Deleted: is

5. (Original) A public-key encryption process according to claim 1, for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key *a*; and

b) calculating a sender public key $A = aG$, where *G* is a generator,

and at the receiver,

a) generating a receiver private key *b*; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key *B* and the receiver obtains an authentic copy of the sender public key *A*.

6. (Currently Amended) A public-key encryption process according to claim 5, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key *x* and calculating [[an]]the encryption ephemeral public key $X = xG$.

7. (Original) A public-key encryption process according to claim 6, further comprising the steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message.

8. (Original) A public-key encryption process according to claim 7, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

9. (Cancelled)

10. (Currently Amended) A public-key encryption process according to claim 8, further comprising the steps of, at the receiver, generating the secret key K by calculating one of: [[=]] bX_x [[=]] bxG_x [[=]] xbG_x *and* [[=]] xB[[,]] and decrypting the transmitted ciphertext message using the generated secret key K_x

Deleted: 9

Deleted: , calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s

11. (Previously Presented) A public-key encryption process according to claim 1, implemented in a wireless communication system;

wherein at least a two stage public-key encryption process is used;

wherein the first stage includes key establishment and the second stage includes encryption/decryption;

wherein said steps (a) and (b) are performed during the second stage of encryption.

12. (Original) A public-key encryption process according to claim 1, implemented in a wireless hand-held communication device.

13. (Original) A public-key encryption process according to claim 1, implemented in a personal digital assistant.

14. (Original) A public-key encryption process according to claim 1, implemented in a cellular phone.

15. (Original) A public-key encryption process according to claim 1, implemented in a two-way pager.

16. (Currently Amended) A public-key encryption system for communicating messages between a sender device and a receiver device, comprising:

a) means, for each message, for encrypting a plaintext message into a ciphertext message, the means for encrypting producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver;

Formatted: Indent: Left: 0 pt, First line: 0 pt

Deleted: and

b) means, for each message, for generating a digital signature using the ephemeral key pair produced by the encrypting means, wherein the digital signature comprises a first value *r* and a second value *s*; and

Deleted: wherein the ephemeral key pair used by the encrypting and generating means is used for a single message between the sender and the receiver

c) means for transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;

wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*.

17. (Original) A public-key encryption system according to claim 16, wherein the means for encrypting employs an E1 Gamal encryption scheme.

18. (Previously Presented) A public-key encryption system according to claim 16, wherein the means for generating a digital signature generates the digital signature using a Nyberg-Rueppel digital signature scheme.

19. (Currently Amended) A public-key encryption system according to claim 16, wherein the means for encrypting produces the ephemeral key pair by generating

an encryption ephemeral private key x and calculating [[an]]the encryption ephemeral public key X = xG in a finite cyclic group having G as a generator.

Deleted: where
Deleted: is

20. (Original) A public-key encryption system according to claim 16, for encrypting messages for communication between a sender and a receiver, the system further comprising, at the sender,

a) means for generating a sender private key a; and

b) means for calculating a sender public key A = aG, where G is a generator, and at the receiver,

a) means for generating a receiver private key b; and

b) means for calculating a receiver public key B = bG,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains authentic copy of the sender public key A.

21. (Currently Amended) A public-key encryption system according to claim 20, wherein the means for encrypting produces the ephemeral key pair by generating an encryption ephemeral private key x and calculating [[an]]the encryption ephemeral public key X = xG.

22. (Original) A public-key encryption system according to claim 21, wherein the means for encrypting generates a secret key K = xB and uses the secret key K to encrypt a plaintext message and thereby generate a ciphertext message.

23. (Previously Presented) A public-key encryption system according to claim 22, wherein the means for generating uses the encryption private key x as a signature ephemeral private key and uses the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature.

24. (Cancelled)

25. (Currently Amended) A public-key encryption system according to claim 23, further comprising, at the receiver, means for decrypting a ciphertext message, wherein the means for decrypting generates the secret key K = bX and decrypts the transmitted ciphertext message using the generated secret key K[[s]].

26. (Original) A public-key encryption system according to claim 16, implemented in a wireless communication system.

27. (Original) A public-key encryption system according to claim 16, implemented in a wireless hand-held communication device.

28. (Original) A public-key encryption system according to claim 16, implemented in a personal digital assistant.

Deleted: 24

Deleted: and means for validating a digital signature

Deleted: , and the means for validating calculates the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validates the digital signature based on the calculated first value r and the transmitted second value

29. (Original) A public-key encryption system according to claim 16, implemented in a cellular phone.

30. (Original) A public-key encryption system according to claim 16, implemented in a two-way pager.

31. (Currently Amended) A software program on a computer-readable storage medium, which when executed by a processor performs a public-key encryption process for communicating messages between a sender and a receiver comprising the steps of:

for each message:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver; and

b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encryption step, wherein the digital signature comprises a first value *r* and a second value *s*; and

c) transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;

Deleted: and

Deleted: wherein the ephemeral key pair used in the encrypting and generating steps is used for a single message between the sender and the receiver

wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and validating the digital signature based on the calculated first value *r* and the transmitted second value *s*.

32. (Original) A software program according to claim 31, wherein the encrypting step uses an El Gamal encryption scheme.

33. (Previously Presented) A software program according to claim 31, wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme.

34. (Currently Amended) A software program according to claim 31, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key *x* and calculating [[an]]the encryption ephemeral public key $X = xG$, in a finite cyclic group having *G* as a generator.

Deleted: ,
Deleted: where
Deleted: is

35. (Original) A software program according to claim 31, for encrypting messages for communication between a sender and a receiver, the software program performing the further steps of, at the sender,

a) generating a sender private key *a*; and

b) calculating a sender public key $A = aG$, where *G* is a generator,

and at the receiver,

a) generating a receiver private key *b*; and

b) calculating a receiver public key $B = bG$,

wherein the sender obtains an authentic copy of the receiver public key *B* and the receiver obtains an authentic copy of the sender public key *A*.

36. (Currently Amended) A software program according to claim 35, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key *x* and calculating [[an]]the encryption ephemeral public key $X = xG$.

37. (Original) A software program according to claim 36, wherein the software program performs the further steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key *K* to generate a ciphertext message.

38. (Original) A software program according to claim 37, wherein the software program performs the further steps of, at the sender, using the encryption private key *x* as a signature ephemeral private key and using the encryption ephemeral public key *X* as a signature ephemeral public key to generate a digital signature.

39. (Cancelled)

40. (Currently Amended) A software program according to claim 38, the software program performing the steps of, at the receiver, generating the secret key *K* by calculating one of: [=] *bX*, [[=]]*bxG*, [[=]]*xbG*, *and* [[=]]*xB*[[,]]and decrypting the transmitted ciphertext message using the generated secret key *K*.

Deleted: 39

Deleted: , calculating the first value *r* of the digital signature using the decrypted message and the transmitted encryption ephemeral public key *X* and validating the digital signature based on the calculated first value *r* and the transmitted second value *s*

41. (Original) A software program according to claim 31, installed in a wireless communication system.

42. (Original) A software program according to claim 31, installed in a wireless hand-held communication device.

43. (Original) A software program according to claim 31, installed in a personal digital assistant.

44. (Original) A software program according to claim 31, installed in a cellular phone.

45. (Original) A software program according to claim 31, installed in a two-way pager.

Allowable Subject Matter

Claims 1-8, 10-23, 25-38 and 40-45 are allowed.

The following is an examiner's statement of reasons for allowance:

The present invention is directed towards a public-key encryption process, system, and software program for communicating messages between a sender and receiver. Independent claims 1, 16, and 31 each identify the uniquely distinct feature of:

- encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message, wherein the ephemeral key pair is used for a single message between the sender and the receiver;
- generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step, wherein the digital signature comprises a first value *r* and a second value *s*;
- transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature to the receiver;
- wherein the first value r of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*

The closest prior art, US Patent No. 5,956,404to Schneier discloses a public-key encryption process, system, and software program for communicating messages between a sender and a receiver as well as the general use of ephemeral key pairs.

Nowhere does Schneier disclose transmitting, from the sender, an encryption ephemeral public key *X* of the ephemeral key pair, the ciphertext message, and the second value *s* of the digital signature generated using the ephemeral key pair produced in the encrypting step to the receiver, wherein the first value *r* of the digital signature is calculated at the receiver using a decrypted form of the plaintext message and the transmitted encryption ephemeral public key *X* and the digital signature is validated based on the calculated first value *r* and the transmitted second value *s*.

The prior art, either singularly or in combination fails to anticipate or render obvious the present invention.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437